CLAIMS

1. A network system, comprising:

a first device to maintain an original resource;

a second device to maintain a replica resource remotely from the first device, the replica resource being replicated from the original resource;

memory to store a cached descriptor corresponding to the original resource;

a security component to determine whether the replica resource will pose a security risk to the second device upon receipt of a request for the replica resource, the security component:

formulating a descriptor corresponding to the replica resource and comparing the formulated descriptor with the cached descriptor; and

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to the original resource and comparing the formulated descriptor with the second descriptor.

2. A network system as recited in claim 1, wherein the security component determines that the replica resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

3. A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are equivalent, the security component determines that the replica resource is not a security risk.

4. A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are equivalent, the security component determines that the replica resource is not a security risk, and the cached descriptor is replaced with the second descriptor.

5. A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent, the security component determines that the replica resource is a security risk, and the replica resource is replaced with a copy of the original resource.

6. A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent, the security component determines that the replica resource is a security risk, the replica resource is replaced with a copy of the original resource, and the cached descriptor is replaced with the second descriptor.

7. A network system as recited in claim 1, wherein the security component formulates the cached descriptor when the original resource is replicated to create the replica resource.

8. A network system as recited in claim 1, wherein the security component is configured to determine whether the request will pose a security risk to the second device.

9. A network system as recited in claim 8, wherein the request designates a resource locator.

10. A network system as recited in claim 8, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the replica resource, and wherein the security component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

11. A network system as recited in claim 8, wherein the request designates a resource locator having a plurality of arguments, and wherein the security component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

12. A network system as recited in claim 8, wherein the request designates a resource locator having a resource identifier, and wherein the security component determines that the request is not a security risk if the resource identifier has a valid file extension.

13. A network system as recited in claim 1, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the replica resource and the resource path having a resource identifier;

the security component is configured to determine whether the request will pose a security risk to the second device;

the security component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

14. A network server, comprising:

a server component to receive a request for a resource maintained on the network server and, in response to the request, implement security policies to prevent unauthorized access to the resource; and

a security component that is registerable with the server component during run-time to determine whether the request will pose a security risk to the network server.

15. A network server as recited in claim 14, wherein, if the security component determines that the request will pose a security risk, the security component redirects the request to indicate that the resource is not available.

16. A network server as recited in claim 14, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the security component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

17. A network server as recited in claim 14, wherein the request designates a resource locator having a plurality of arguments, and wherein the security component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

18. A network server as recited in claim 14, wherein the request designates a resource locator having a resource identifier, and wherein the security component determines that the request is not a security risk if the resource identifier has a valid file extension.

19. A network server as recited in claim 14, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the security component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

20. A network server, comprising:

a server component to receive a request for a resource maintained on the network server and, in response to the request, implement security policies to prevent unauthorized access to the resource; and

a security component that is registerable with the server component during run-time to determine whether the resource will pose a security risk to the network server upon receipt of the request.

21. A network server as recited in claim 20, wherein, if the security component determines that the resource will pose a security risk, the security component redirects the request to indicate that the resource is not available.

22. A network server as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested; and

determines that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

23. A network server as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor; and

determines that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

24. A network server as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor;

if the formulated descriptor and the second descriptor are not equivalent, initiates that the resource stored on the network server be replaced with a copy of the original resource maintained on the file server; and

initiates that the cached descriptor be replaced with the second descriptor.

25. A network server, comprising:

an Internet server to receive a request for a resource maintained on the network server and, in response to the request, implement security policies to prevent unauthorized access to the resource;

a security component that is registerable with the Internet server during run-time, the security component having:

a validation component to determine whether the request will pose a security risk to the network server; and

an integrity verification component to determine whether the resource will pose a security risk to the network server upon receipt of the request.

26. A network server as recited in claim 25, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the validation component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

27. A network server as recited in claim 25, wherein the request designates a resource locator having a plurality of arguments, and wherein the validation component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

28. A network server as recited in claim 25, wherein the request designates a resource locator having a resource identifier, and wherein the validation component determines that the request is not a security risk if the resource identifier has a valid file extension.

29. A network server as recited in claim 25, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the validation component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

30. A network server as recited in claim 25, wherein the integrity verification component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested; and

determines that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

31. A network server as recited in claim 25, wherein the integrity verification component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor; and

determines that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

32. A network server as recited in claim 25, wherein the integrity verification component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor;

if the formulated descriptor and the second descriptor are not equivalent, initiates that the resource stored on the network server be replaced with a copy of the original resource maintained on the file server; and

initiates that the cached descriptor be replaced with the second descriptor.

33. A computing device, comprising:

an operating system to access resources to service requests;

a security component to determine whether a resource will pose a security risk to the computing device upon receipt of a request to access the resource;

the security component configured to:

formulate a descriptor corresponding to the resource;

retrieve a cached descriptor corresponding to the resource, the cached descriptor stored on a remote second computing device;

compare the formulated descriptor with the cached descriptor; and

determine that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

34. A computing device as recited in claim 33, wherein the security component formulates the cached descriptor when the resource is initially requested.

35. A computing device as recited in claim 33, wherein the security component initiates a remote data server to formulate the cached descriptor and store the cached descriptor on the remote second computing device when the resource is stored on the computing device.

36. A computing device as recited in claim 33, wherein, if the formulated descriptor and the cached descriptor are not equivalent, the security component initiates that the resource be replaced with a copy of the resource maintained on the remote second computing device.

37. One or more computer readable media containing a security application, comprising:

a validation component to determine whether a request for a resource poses a security risk; and

an integrity verification component to determine whether the resource poses a security risk.

38. Computer readable media as recited in claim 37, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the validation component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

39. Computer readable media as recited in claim 37, wherein the request designates a resource locator having a plurality of arguments, and wherein the validation component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

40. Computer readable media as recited in claim 37, wherein the request designates a resource locator having a resource identifier, and wherein the validation component determines that the request is not a security risk if the resource identifier has a valid file extension.

41. Computer readable media as recited in claim 37, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the validation component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

42. Computer readable media as recited in claim 37, wherein the integrity verification component:

formulates a descriptor corresponding to the resource when the security application receives the request;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested; and

determines that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

43. Computer readable media as recited in claim 37, wherein the integrity verification component:

formulates a descriptor corresponding to the resource when the security application receives the request;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource remotely located, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor; and

determines that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

44. Computer readable media as recited in claim 37, wherein the integrity verification component:

formulates a descriptor corresponding to the resource when the security application receives the request;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource remotely located, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor;

if the formulated descriptor and the second descriptor are not equivalent, initiates that the resource be replaced with a copy of the original resource; and

initiates that the cached descriptor be replaced with the second descriptor.

45. A method, comprising:

receiving a request for a replica resource stored on a computing device;

formulating a descriptor corresponding to the replica resource;

comparing the formulated descriptor with a cached descriptor corresponding to an original resource stored on a second computing device remotely located from the computing device, the replica resource being replicated from the original resource;

determining that the replica resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to the original resource;

comparing the formulated descriptor with the second descriptor; and

determining that the replica resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent.

46. A method as recited in claim 45, further comprising allowing the request if said determining that the replica resource does not pose a security risk to the computing device.

47. A method as recited in claim 45, further comprising redirecting the request to indicate that the replica resource is not available if determining that the replica resource poses a security risk to the computing device.

48. A method as recited in claim 45, further comprising replacing the cached descriptor with the second descriptor if the formulated descriptor and the second descriptor are equivalent.

49. A method as recited in claim 45, further comprising replacing the replica resource with a copy of the original resource if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent.

50. A method as recited in claim 45, further comprising replacing the cached descriptor with the second descriptor if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent.

51. A method as recited in claim 45, further comprising formulating the cached descriptor when the original resource is replicated to create the replica resource.

52. A method as recited in claim 45, further comprising formulating the cached descriptor when the replica resource is initially requested.

53. A method as recited in claim 45, further comprising determining whether the request will pose a security risk.

54. A method as recited in claim 45, further comprising:

determining whether the request will pose a security risk; and

redirecting the request to indicate that the replica resource is not available if determining that the request poses a security risk to the computing device.

55. A method as recited in claim 45, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the replica resource, and the method further comprising determining that the request does not pose a security risk if the resource path does not exceed a maximum number of characters.

56. A method as recited in claim 45, wherein the request designates a resource locator having a plurality of arguments, and the method further comprising determining that the request does not pose a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

57. A method as recited in claim 45, wherein the request designates a resource locator having a resource identifier, and the method further comprising determining that the request does not pose a security risk if the resource identifier has a valid file extension.

58. A method as recited in claim 45, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the replica resource and the resource path having a resource identifier;

the method further comprising determining that the request does not pose a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

59. A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 45.

60. A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 58.

61. A method, comprising:

receiving a request for a resource;

implementing security policies to prevent unauthorized access to the resource;

determining whether the request will pose a security risk; and

determining whether the resource will pose a security risk if allowing the request.

62. A method as recited in claim 61, further comprising allowing the request for the resource if determining that the request does not pose a security risk and if determining that the resource does not pose a security risk.

63. A method as recited in claim 61, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and the method further comprising determining that the request does not pose a security risk if the resource path does not exceed a maximum number of characters.

64. A method as recited in claim 61, wherein the request designates a resource locator having a plurality of arguments, and the method further comprising determining that the request does not pose a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

65. A method as recited in claim 61, wherein the request designates a resource locator having a resource identifier, and the method further comprising determining that the request does not pose a security risk if the resource identifier has a valid file extension.

66. A method as recited in claim 61, further comprising:

formulating a descriptor corresponding to the resource;

comparing the formulated descriptor with a cached descriptor corresponding to the resource and formulated when the resource is initially requested; and

determining that the resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent.

67. A method as recited in claim 61, further comprising:

formulating a descriptor corresponding to the resource;

comparing the formulated descriptor with a cached descriptor corresponding to the resource and formulated when the resource is initially requested;

determining that the resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to an original resource remotely located, the resource replicated from the original source;

comparing the formulated descriptor with the second descriptor; and

determining that the resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent.

68. A method as recited in claim 61, further comprising:

formulating a descriptor corresponding to the resource;

comparing the formulated descriptor with a cached descriptor corresponding to the resource and formulated when the resource is initially requested;

determining that the resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to an original resource remotely located, the resource replicated from the original resource;

comparing the formulated descriptor with the second descriptor; and

determining that the resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent;

if the formulated descriptor and the second descriptor are not equivalent, replacing the resource with a copy of the original resource and replacing the cached descriptor with the second descriptor.

69. A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 61.

70. A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 68.

71. A method to determine whether an operating system can access a resource without a security risk, the method comprising:

formulating a descriptor corresponding to the resource;

retrieving a cached descriptor corresponding to the resource, the cached descriptor stored remotely;

comparing the formulated descriptor with the cached descriptor; and

determining that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

72. A method as recited in claim 71, further comprising allowing the operating system to access the resource if said determining that the resource is not a security risk.

73. A method as recited in claim 71, further comprising formulating the cached descriptor when the resource is created.

74. A method as recited in claim 71, further comprising formulating the cached descriptor when the resource is initially requested.

75. A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 71.